Appendix TOM

Minimum technical and organizational measures

for service providers of Arvato Systems

Version 4.0

Public

Disclaimer

Contents

1 Agreement on concrete technical and organizational measures

The technical and organizational measures concretely implemented by the Contractor result from

- the main contract including all appendices such as the service descriptions of the main contract as well as additionally
- the minimum technical and organizational measures in section 2, whereby the respective applicable type of access (see 1.1) is to be derived from the main contract.

1.1 Definition type of access

The set of minimum measures to be fulfilled depends on the type of the Contractor's access to the Client's data. The type of access is defined in the following table.

Type	Brief description of the type	Definition of the type of access
A	Contractor provides a core service on its own IT systems	The Contractor's access to Client's data falls neither into type B, not C, nor D.
B	Contractor obtains access to IT systems provided by Arvato Systems via Contractor's end devices	In order to provide the service, the Contractor will be granted access to the IT systems provided by the Client and will use Contractor's end devices for such access. There will be no processing of personal data on behalf of the Client on the Contractor's IT systems outside the end devices.
C	Contractor obtains access to IT systems provided by Arvato Systems via Arvato Systems' end devices	In order to provide the service, the Contractor will be granted access to the IT systems provided by the Client and will use Client's end devices for such access. There will be no processing of personal data on behalf of the Client on the Contractor's IT systems.
D	Contractor only receives log files without access to Arvato System's IT systems	Only extracts of pseudonymized meta/log data of normal protection level from Client's IT systems will be transmitted to the Contractor in order to ensure the confidentiality, availability, integrity or resilience of the IT systems. The Contractor has no access to Client's IT systems.

2 Minimum technical and organizational measures

The following technical and organizational measures are minimum standards for processing personal data on behalf of the Client and apply to assets, systems, and processes for which the Contractor is the owner or is defined in the contract as "accountable (= responsible for the performance or makes related decisions)".

2.1 Minimum measures

The following table lists the required minimum measures per type of access (see definition 1.1 for type A, B, C or D). If the Contractor also performs activities for the provision of services from the home office or by mobile working, the measures in chapter 2.2 must also be fulfilled.

No.	Measure	A	B	C	D
1. Organization of Data Protection and Information Security					
1.1	Rules and regulations exist for information security and data protection.	x			x
1.2	The rules and regulations for information security and data protection are regularly reviewed for compliance and effectiveness.	x			x
1.3	The security concepts and measures and their implementation are reviewed regularly.	x	x	x	x
1.4	A person is designated who is responsible for overall compliance with these technical and organizational security measures.	x	x	x	x
2. Human Resources Security					
2.1	Employees go through a starter-changer-leaver process, which takes into account security requirements when filling, changing and terminating jobs.	x	x	x	x
2.2	Employees are committed to observe data protection secrecy.	x	x	x	x
2.3	Employees are regularly trained on data protection and information security.	x	x	x	x
2.4	Instructions are established for handling, processing and forwarding of information, the use of mobile devices and storage media as well as the design of working environments (acceptable use policy, clean desk policy).	x	x	x	x
3. Asset Management					
3.1	Processes to maintain an asset inventory and records of processing activities are defined and established.	x	x		x
3.2	Specifications for the classification of data into different protection levels are established.	x			x
3.3	Transports of data storage devices containing personal data are subject to a control and documentation process. Data storage devices are transported outside the area of the company in secured, locked transport containers by special courier services or secured with procedures such as encryption.	x			x
3.4	Procedure for the disposal of devices, data storage devices and confidential documents is established which include specifications for the deletion of information or destruction by specialized and certified companies in accordance with current standards.	x	x		x
4. Physical and Environmental Security					
4.1	Physical security controls for offices, rooms, and facilities are designed and implemented.	x	x		x
4.2	There is a documented procedure for granting, changing, and withdrawing physical access rights, including the return of access equipment.	x	x		x
4.3	Security areas (areas with higher security requirements) are defined, divided into security zones and documented together with the physical protection measures in a security zone concept.	x			x
4.4	Secure areas are protected by appropriate access controls and physical barriers depending on the security zone according to the security zone concept. Access to security zones is controlled and approved to allow access to authorized persons only. Access controls that allow visitors to enter security zones are defined.	x			x
4.5	Access to the Contractor's Data Centers is tracked via a personally assigned means of access with two-factor authentication or comparable protection method.	x			x
4.6	All visitors to the Contractor's Data Centers are recorded with the date and time of their entry and exit and are escorted by authorized personnel.	x			x
4.7	Contractor's Data Centers are physically secured, protected with intrusion alarm systems, and entrances are monitored with video systems.	x			x

No.	Measure	A	B	C	D
4.8	Contractor's Data Centers are protected from technical impairments, and elementary environmental hazards - in particular fire, water, failure of supply networks (e.g., UPS, emergency power system, fire extinguisher, fire detection, etc.). Any deviations from normal operation can be quickly detected and remedied.	x			x
4.9	Contractor's Data Center infrastructure is maintained according to the manufacturer's specifications.	x			x
4.10	Physical assets and server systems are located in a security zone that meets their protection requirements.	x			x
5. System Access Control					
5.1	Within the Identity & Access Management, processes for the allocation, modification and withdrawal of accounts and access rights are documented and in place.	x			x
5.2	Request for access creation or modification are documented and approved by the relevant approver.	x			x
5.3	Each account is always linked to a specific natural person.	x			x
5.4	Accounts and credentials can be blocked immediately.	x			x
5.6	Measures are implemented for the protection of user/password authentication.	x	x		x
5.7	Passwords of sufficient complexity and length are used. The structure and handling of passwords shall be in accordance with a documented password policy.	x	x	x	x
5.8	Default passwords are changed immediately after installation. Initial passwords are individualized.	x			
5.9	Separate accounts/roles and credentials are issued for administrator activities. Administrator accounts are not used for normal office activities.	x			x
5.10	Administrator activities with privileged access rights in Contractor's Data Center are carried out via jump servers, virtual desktops in the Data Center and a PAM (Privileged Access Management) system.	x			
5.11	By default, devices and sessions are locked automatically after a defined period of inactivity.	x	x		x
5.12	All access to systems (mobile devices, applications, operating systems, BIOS, boot devices, etc.) is protected or blocked.	x	x		x
6. Data Access Control					
6.1	Only those access rights are granted that are required to fulfil the respective task (need-to-know and least-privilege principle).	x			x
6.2	Granted access rights are reviewed in regular intervals defined by the criticality of the access rights in scope. Active reapproval is required for high critical accounts. Access rights are revoked as soon as they are no longer required	x			x
6.3	Role-based access controls are implemented in all systems/applications.	x			x
7. Encryption					
7.1	Data on mobile devices is encrypted according to the state of the art and protected against undetected manipulation.	x	x		x
7.2	Data is protected against unauthorized disclosure and manipulation when transported over public networks. (e.g., transport encryption via TLS).	x	x	x	x
7.3	To support cryptographic measures and techniques, an appropriate cryptographic key management is implemented.	x			
7.4	Implemented cryptographic controls are in line with best practices. Insecure (outdated) techniques are timely replaced.	x			x

No.	Measure	A	B	C	D
7.5	The specifications for encrypting the data are agreed between the client and the contractor prior to implementation and specified in the service specifications.	x			
7.6	Where appropriate, data-at-rest is encrypted.	x			x
8. Pseudonymization					
8.1	The specifications for pseudonymization are agreed between the client and the contractor prior to implementation and are specified in the service specifications.	x			
9. Operations					
9.1 Operations - Change Control					
9.1.1	Part of a new or to be changed processing activity is an assessment of the risks of the data subjects and, depending on this, the identification and implementation of technical and organizational security measures.	x			x
9.1.2	The IT operating procedures are documented in a comprehensible manner, are regularly checked, and adjusted if necessary.	x			
9.1.3	Changes to information processing systems are subject to a change management process.	x			x
9.1.4	Rules for software installation and configuration by users on notebooks are defined, implemented, and monitored.	x			x
9.1.5	To decrease the risk of misuse of supporting assets, the authorization and execution of operational procedures are segregated by different roles.	x			x
9.2 Operations - Separation Control					
9.2.1	Personal data of clients are processed in such a way that the client can be identified in the processing. Thus, the data of different clients are always physically or logically separated.	x			x
9.2.2	Development, test, and production environments are separated.	x			x
9.3 Operations - Protection against Malware and Vulnerabilities, Patch Management					
9.3.1	Up-to-date protection against malware and malicious activities is installed and activated on all relevant information systems and mobile devices.	x	x		x
9.3.2	For all systems, new security updates and patches are applied in a timely manner, considering system dependencies, the impact on ongoing operations as well as the damage impact of a vulnerability and the threat exposure.	x	x		x
9.3.3	Software is installed according to specified configuration and hardening standards.	x	x		x
9.3.4	Information is obtained about technical vulnerabilities of information systems in operation. For all systems the exposure to vulnerabilities is evaluated regularly depending on system criticality. Appropriate remedial measures are taken to counteract the exploitation of technical vulnerabilities.	x			x
9.3.5	Penetration tests are planned and performed in defined intervals based on the criticality and exposure of the systems in scope.	x			
9.4 Operations - Availability					
9.4.1	The specifications for Client's Data (Back-up and recovery, redundant systems, geo-redundant Data Center, etc.) are agreed between the client and the contractor prior to implementation and specified in the service specifications.	x			
9.4.2	Backup and recovery procedures are tested regularly, especially after changes to the backup configuration.	x			
9.4.3	A process is established to test redundant systems regarding availability requirements.	x			

No.	Measure	A	B	C	D
9.5 Operations - Network					
9.5.1	The Contractor's network is managed appropriately to protect the information in systems and applications. It is divided into different zones.	x	x		x
9.5.2	External access (remote access) to Contractor's networks and systems is secured and encrypted and requires two-factor authentication.	x			
9.5.3	Only sufficiently secured mobile devices are granted access to the Contractor's network.	x			
9.6 Operations - Logging and Monitoring					
9.6.1	Logs recording activities (incl. administrative activities), exceptions, errors, and other relevant events are produced and stored. The level of detail of the logs is determined by the sensitivity of the information and the criticality of the system, and allows to track inputs and changes of personal data.	x	x		
9.6.2	Network traffic between the network zones is logged and monitored.	x			
9.6.3	Event messages generated on the notebooks for the detection of information security incidents are transmitted to central servers for evaluation.	x			
9.6.4	Log equipment and log data under the accountability of the Contractor is protected against unauthorized access, modification, and deletion.	x			
9.6.5	The clocks of critical systems are synchronized with a reliable and agreed time source.	x			
9.6.6	The degree of monitoring of system and network resources is determined in line with a risk assessment.	x	x		x
9.6.7	Roles and responsibilities for protection against cyber threads are defined and implemented (Security Operations Center). Log data is analyzed for security events.	x			
10. Acquisition, Development and Maintenance of IT Systems					
10.1	There are specifications for software development and the acquisition of IT systems and IT services that include the aspects of IT security and data protection by design and by default.	x			x
11. Supplier Management					
11.1	Agreements on the exchange of information are concluded and consider the security of information.	x	x	x	x
11.2	Prior to engaging external subcontractors, an assessment of the risks regarding data protection and information security is carried out in relation to their future tasks. The selection of a suitable subcontractor is based on the results of this assessment.	x	x	x	
11.3	Compliance with the data processing agreements is assessed and reviewed regularly.	x	x	x	x
12. Information Security and Data Protection Incident Management					
12.1	Processes for identifying, assessing, and handling security and data protection incidents are in place and trained.	x			x
12.2	Central functions are responsible for coordinating and responding to information security and data protection incidents, performing the assessment, and deciding on the classification of incidents.	x			
12.3	In the event of a data breach, a notification must be sent immediately to the e-mail address Datenschutz@arvato-systems.de, with the necessary information required by law.	x	x	x	x
13. Business Continuity Management					
13.1	There is a documented business continuity management procedure. Processes and responsibilities are defined to carry out the crisis management and corresponding exercises take place regularly.	x			x

2.2 Minimum measures for mobile working or home office

The following table lists the minimum measures required in addition to chapter 2.1, which must be fulfilled if the Contractor performs activities for the provision of services from the home office or by mobile working.

No.	Measure	A	B	C	D
2. Human Resources Security					
2.5	Employees are instructed and trained to adequately protect company information, especially in the mobile work environment - from unauthorized third parties viewing the screen by using privacy film and locking of mobile devices when not in use - from unauthorized third parties viewing work documents/printouts through a clean desk policy - from unauthorized third parties taking note of confidential conversations or telephone calls - by keeping mobile devices and equipment appropriately safe - by compliant disposal of paper and data storage devices. Compliance with the instructions can be checked by the employer.	x	x	x	x
5. System Access Control					
5.4	Accounts and credentials can be blocked immediately.	x	x		x
5.5	Conformity of mobile devices with defined policies is monitored. In case of non-compliance, access is denied.	x			x
5.13	Employees use company-provided hardware and software, including standard communications software, for work-related activities. Exception for mobile working: Devices required for the Internet connection and, if necessary, own peripheral devices (e.g., printer, monitor, mouse, keyboard), if these have been purchased as common brand devices from a trustworthy source.	x	x		x
9.5 Operations - Network					
9.5.3	Only sufficiently secured mobile devices are granted access to the Contractor's network.	x	x		x
9.6 Operations - Logging and Monitoring					
9.6.3	Event messages generated on the notebooks for the detection of information security incidents are transmitted to central servers for evaluation.	x	x		x